UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

9

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,665	02/02/2001	Donald B. Johnson	6944-8-1	7060

293 7590 05/16/2006

Ralph A. Dowell of DOWELL & DOWELL P.C.
2111 Eisenhower Ave
Suite 406
Alexandria, VA 22314

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/773,665	**Applicant(s)** JOHNSON ET AL.	
	Examiner Paula W. Klimach	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *12-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-21* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *02/02/01*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/09/06 has been entered.

Response to Arguments

Applicant's arguments filed 03/09/06 have been fully considered but they are not persuasive because of following reasons.

Applicant argued that instance s` in claim 12 is derived from components s and c, which are derived as outlined above. This is not found persuasive. The applicant has not claimed that s` is derived form s and c. The claim 12 clearly states "s` being derived from said fist and second signature components." In the preamble the applicant recites, "said sender generating masked signature components (r, s, c)." The applicant has not claimed the first signature component and stated that c is a second component. The examiner assumed that the applicant meant r is a first component, s is a second component and c is a thirds component, since there is no mention in the preamble or any other section of the first signature component. Therefore s`, in this system would be composed of r and s. Correction of the preamble or amendment to the limitation would clarify the applicant's invention.

In reference to the applicant's argument, "component c is derived from the first and second short term private keys. A careful review of Schneier will reveal that there is no mention of deriving a signature component in such a way." This is not found persuasive because of the lack of a first signature component as disclosed in the arguments above. Even if the first component was r and the second component was c, then d corresponds to s`, since s is then derived from r and c (wherein c is derived from the first and second short term private keys), D is derived from n which is calculated from two secret primes. Private keys are values that are prime and secret. The secret primes are short term since they are used for the message between Peggy and Victor, which is a short term.

The applicant argued further that Schneier does not teach obtaining a pair of signature components from a set of three components as recited in claim 12. This is not found persuasive. The claim 12 does not recite obtaining a pair of signature components form a set of three components. Due to the discrepancy disclosed above, the signature is either calculated from r and s or r and c. These are two components. The claim does not recite, "the verifier obtains (s`, r) from (r, s, c)."

The applicant argued further that the examiner does not even provide an explanation as to where Koyama provides any direction or motivation to jump form the mere presence of elliptic curves to incorporating an undisclosed step into the teachings of Schneier relating to a specific signature scheme. This is not found persuasive. The motivation for combination of the teachings of Shneier with the teachings of Koyama is given in the rejection below. The teaching of Schneier would use the elliptic curve of Koyama because "the computational speed of the elliptic curve algorithm is faster than that of RSA and therefore for the analogues of RSA."

Wherein the system disclosed by Schneier is an analogue of RSA (Guillou-Quisquater Identification Scheme page 509 paragraph 1; public key).

The applicant argued further that neither Schneier nor Koyama teach recovering a coordinate pair that corresponds to a short term public key kP using a pair of signature components. In the combination of Schneier and Koyama, Koyama teaches the short term public key in recovering the coordinates and Schneier teaches s` and r derived from kP.

The examiner asserts that Schneier and Koyama do teach or suggest the subject matter broadly recited in independent Claims 12. Dependent Claims 13-21 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 12-21 are respectfully maintained.

Information Disclosure Statement

The information disclosure statement filed 02/02/06 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 12-13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim recites a method for verifying a signature, the method being is a process containing mathematical algorithms that do not produce a useful, concrete and tangible result. The result of the method is a compare algorithm that compares r\` to r. There is no data that is output to a screen or printed or in anyway output to the outside world, it remains in the apparatus. The result is non-statutory subject matter.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: defining the elliptic curve over a finite field. This is the elliptic curve that is used to recover a coordinate pair x1, y1. The specification discloses the invention is thus generally concerned with an encryption method and system and <u>particularly an elliptic curve encryption method and system in which finite field elements are multiplied in a processor efficient manner (page 8 lines 10-13).</u> Even though the specification discloses the importance of the elliptic curve multiplication over a finite field, the claims are silent as to the important step required to recover the coordinates x1 and y1.

Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims recites s being derived from said first and second signature components however, the claim does not disclose what the first signature component is.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 12-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applied Crytography by Schneier in view of the article "New Public-Key Schemes Based on Elliptic Curves over the Ring Zn" by Koyama.

In reference to claim 12, Schneier discloses a system wherein the verifier (Bob) obtaining a pair of signature components (d, D), said component being derived from a first (random integer r) and second signature components (B) generated by a signor; the verifier (Bob) calculating a signature component r' (d`) from one of said coordinate pairs; and verifying said signature if r' = r (d = d`; pages 509-510 Guillou-Quisquater Signature Scheme).

The signature scheme of Guillou-Quisquater does not disclose the use of elliptic curve for calculating the signature.

Koyama discloses the use of elliptic curve to calculate digital signatures and therefore the recovering of a coordinate pair (x1,y1) corresponding to said first short term public key using the pair (s, t) and said message M (Section 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use elliptic curve as in Koyama in the system of Schneier. One of ordinary skill in the art would have been motivated to do this because the computational speed of the elliptic curve algorithm is faster than that of RSA and therefore for the analogues of RSA.

In reference to claim 13 further comprising the step of said verifier receiving (r, s, c) from said signor and converting (s, r, c) to obtain said pair (s, r) (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 14, further comprising the step of said signor converting (s, r, c) to said pair (s,r) and said signor sending said pair (s, r) to said verifier.

Schneier discloses the verifier receiving the three components and converting these into two components (pages 509-510 Guillou-Quisquater Signature Scheme).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to convert the components by the signor. One of ordinary skill in the art would have been motivated to do this because it is a mere calculation that can be performed at either device.

In reference to claim 15 wherein said coordinate pair (x1,y1) is calculated using a pair of values u and v, said values u and v derived from said pair (s,r) and said message

Koyama discloses the use of elliptic curve to calculate digital signatures and therefore the recovering of a coordinate pair (x1,y1) corresponding to said first short term public key using the pair (s, t) and said message M (Section 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use elliptic curve as in Koyama in the system of Schneier. One of ordinary skill in the art would have been motivated to do this because the computational speed of the elliptic curve algorithm is faster than that of RSA and therefore for the analogues of RSA.

In reference to claim 16 wherein said coordinate pair (x1,y1) is calculated as (x1,y1) = uP + vQ, wherein P is a point on an elliptic curve E and Q is a public verification key of said signor derived from P as Q = dP

Koyama discloses the use of elliptic curve to calculate digital signatures and therefore the recovering of a coordinate pair (x1,y1) corresponding to said first short term public key using the pair (s, t) and said message M (Section 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use elliptic curve as in Koyama in the system of Schneier. One of ordinary skill in the art would have been motivated to do this because the computational speed of the elliptic curve algorithm is faster than that of RSA and therefore for the analogues of RSA.

In reference to claim 17 wherein said value u is computed as u = s^{-1} emod n and said value v is computed as v = s r mod n , e being a representation of said, message m (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 18 wherein e is calculated as e=H(m), H( ) being a hash function of said signor and being known to said verifier (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 19 wherein said coordinate x1 first converted to an integer x1 prior to calculating said component r` (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 20 wherein said component r` , is calculated as r'= x1 mod n (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 21 wherein prior to calculating said component r`, said coordinate pair (x1,y1) is first verified, whereby if said coordinate pair (x1, y1) is a point at infinity, then said signature is rejected.

Koyama discloses the use of elliptic curve to calculate digital signatures and therefore coordinate pair (x1, y1) is a point at infinity, then said signature is rejected (Section 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use elliptic curve as in Koyama in the system of Schneier. One of ordinary skill in the art would have been motivated to do this because the computational speed of the elliptic curve algorithm is faster than that of RSA and therefore for the analogues of RSA.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Thursday, May 11, 2006

HOSUK SONG
PRIMARY EXAMINER